(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 944 027 A2

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
22.09.1999 Patentblatt 1999/38

(51) Int Cl.[6]: **G07B 17/00**

(21) Anmeldenummer: **99250071.0**

(22) Anmeldetag: **09.03.1999**

(84) Benannte Vertragsstaaten:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

(30) Priorität: **18.03.1998 DE 19812903**

(71) Anmelder: **Francotyp-Postalia Aktiengesellschaft & Co.**
16547 Birkenwerder (DE)

(72) Erfinder: **Pauschinger, Dieter, Dr.**
16540 Hohen Neuendorf (DE)

(54) Frankiereinrichtung und ein Verfahren zur Erzeugung gültiger Daten für Frankierabdrucke

(57) Eine Frankiereinrichtung (10) für ein kleines Postaufkommen besteht aus einem Computer (11) und mit einem angeschlossenen Drucker (17), wobei der Computer einen Speicher (13) mit einer lokalen Datenbank für Postempfängeradreßdateien über ein Kommunikationsmittel (15) mit einer Datenzentrale (20) verbunden ist, welche eine zentrale Datenbank (23) aufweist. Der Computer (11) ist entsprechend programmiert, daß Anforderungsdaten gebildet und zur Datenzentrale übermittelt und angeforderte zurückübermittelte Daten empfangen und gespeichert werden. Das Verfahren zur Erzeugung gültiger Daten für Frankierabdrucke umfaßt dabei folgende Schritte:

- Bildung und Übermittlung von Anforderungsdaten für eine Signatur,
- Verifikation von übermittelten Daten in einer Datenzentrale (20),
- Erzeugung einer Signatur auf der Basis verifizierter Daten unter Verwendung eines asymmetrischen Kryptoalgorithmus und geheimen privaten Schlüssels, sowie
- Rückübermittlung der verifizierten Daten und der Signatur zur Frankiereinrichtung (10), wobei die Authentizität der zurückübermittelten Daten anhand der Signatur unter Verwendung eines öffentlichen Schlüssels überprüfbar ist, sowie
- Speicherung authentischer empfangener Daten in der lokalen Datenbank (13).

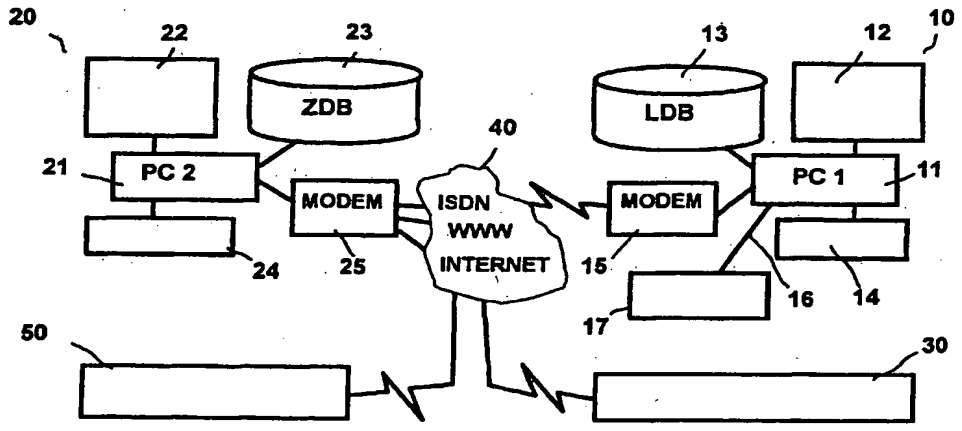

Fig.1

EP 0 944 027 A2

Beschreibung

[0001] Die Erfindung betrifft eine Frankiereinrichtung und ein Verfahren zur Erzeugung gültiger Daten für Frankierabdrucke gemäß des Oberbegriffs des Anspruchs 1 beziehungsweise des Anspruchs 4. Die Frankiereinrichtung ist insbesondere im Heimbereich und für Anwender geeignet, die nur wenig Poststücke versenden.

[0002] In der DE 40 18 166 C2 wurde bereits für solche Anwender mit geringem Postgutaufkommen ein Frankiermodul für einen Personalcomputer vorgeschlagen, in dessen Slot eines Laufwerkeinschubes das Frankiermodul angeordnet ist, welches sowohl das Frankieren als auch das Adressieren von Briefumschlägen gestattet. Ein solches Frankiermodul ist von einem gesicherten Gehäuse umgeben und hat schaltungstechnisch den gleichen Aufbau, wie eine Frankiermaschine, bei welcher die Brieftransportvorrichtung eingespart wird. Es versteht sich von selbst, daß ein derartig abgerüstetes Frankiermodul billiger angeboten werden kann, als eine Frankiermaschine.

[0003] Durch den Einsatz des Frankiermoduls kann die Abrechnung der Frankierung und das Drucken des Frankierstempel-bildes nicht von extern manipuliert werden. Die Adreßdaten werden von einem vom Personalcomputer verwalteten Speicher gelesen und über das interne Informationsnetz dem Frankiermodul zugeführt. Dabei ist allerdings nicht ausgeschlossen, daß fehlerhafte Adreßdaten letztendlich dazu führen, daß der Postbeförderer das Poststück nur schwer oder gar nicht dem Postempfänger zustellen kann. Bei einem digitalen Druckverfahren ist es schwer festzustellen, ob das gedruckte Frankierstempelbild nicht bloß eine unabgerechnete Kopie eines früheren Abdruckes ist und mit einer gewünschten anderen Adresse kombiniert wurde. Deshalb werden spezielle rote fluoreszierenden Tinten vorgeschrieben, welche schwer zu kopieren sind. Durch die inszwischen erreichten Fortschritte bei Farbkopierern und Farbdruckern kann eine derartige Maßnahme nicht mehr als ernst zunehmendes Hindernis gelten, gefälsche unabgerechnete Abdrucke herzustellen.

[0004] Gewöhnlich ist am Personalcomputer auch ein Drucker angeschlossen, mit dem heutzutage nicht nur Briefe ausgedruckt, sondern auch Adressen auf Kuverte gedruckt werden können. Grundsätzlich kann damit auch das Kuvert frankiert werden. Es ist jedoch schwierig bei solchen offenen Systemen eine Manipulation zu verhindern. Über die ungesicherten Verbindungsleitungen, könnte nämlich ein Manipulator in Fälschungsabsicht versuchen, Daten in das System einzuspeisen, indem er vortäuscht, sie kämen von der dazu authorisierten Stelle.

[0005] Die US-Postbehörde hat einen im Jahre 1996 veröffentlichten Katalog mit Anforderungen an die Konstruktion von zukünftigen sicheren Frankiersystemen aufgestellt (Information based Indicia Program IBIP). Darin wird angeregt, bestimmte Daten kryptografisch zu verschlüssen und in Form einer digitalen Unterschrift auf den zu frankierenden Brief zu drucken, anhand derer die Postbehörde die Echtheit von Frankierabdrucken überprüfen kann. Bei der US-Postbehörde entsteht nach geschätzten Angaben durch Betrug ein jährlicher Schaden von ca. 200 Millionen US-$. Diese Anforderungen sind nach Art der Frankiereinrichtung differenziert worden. Traditionelle Frankiermaschinen, welche in der Regel nur einen Frankierstempel in Rot aufdrucken werden auch als "closed systems" bezeichnet und brauchen anders als bei sogenannten "open systems" (PC-Frankierer) die entsprechende Briefadresse nicht in die Verschlüsselung mit einbeziehen. Für open systems ist jedoch weiterhin ein Sicherheitsmodul mit fortschrittlicher Kryptotechnologie und gesichertem Gehäuse vorgeschrieben, in welches Daten der Datenzentrale eingespeichert werden können.

[0006] Aus der US 5.625.839 ist das Senden einer Update-Information als Datenpaket an eine Frankiermaschine bekannt. Mit einer CRC-Prüfsumme kann zwar die Fehlerfreiheit der Datenübermittlung geprüft werden, was jedoch noch nichts über die Richtigkeit des übermittelten Dateninhaltes selbst aussagt. Ein Problem könnte wegen der ungesicherten Verbindungsleitung entstehen, wenn nämlich ein Manipulator in Fälschungsabsicht versucht, Daten in die Frankiermaschine einzuspeichern, indem er vortäuscht, sie kämen von der Datenzentrale.

[0007] In der DE 38 40 041 A1 wurde deshalb bereits eine Anordnung vorgeschlagen, in welcher eine Frankiereinrichtung über eine ständig in Betrieb befindliche TEMEX-Standleitung mit einem Zentralrechner verbunden ist. Der Postkunde gibt in die Frankiereinrichtung den gewünschten Frankierwert ein. Letzterer wird zum Zentralrechner übertragen, welcher mit einem Giro-Rechner verbunden ist, bei welchem der Kunde ein Postgiro-Konto hat. Nach einer Deckungsprüfung nimmt der Giro-Rechner die Abrechnung vor und der Zentralrechner gibt die Frankierfunktion frei. Auch die Frankiereinrichtung selbst besitzt zusätzlich postalische Speicher, welche aufgrund des Datenverbundes abgefragt werden können und eine zusätzliche Sicherheit vor Datenverlust im Falle eines Rechnerausfalls bieten. Der Zentralrechner löst einen Alarm aus, wenn diese Standleitung unerlaubt angezapft oder unterbrochen wird. Es ist allerdings aufwendig und somit nicht überall möglich, eine solche spezielle gesicherte Leitung einzusetzen.

[0008] Aus dem EP 373 971 B1 ist ein Kommunikationssystem bekannt, mit einem Übermitteln von Adressendaten von einer lokalen zu einer zentralen Datenbank in einer Datenzentrale, ein Aktualisieren der gespeicherten Adressendaten in der einer zentralen Datenbank der Datenzentrale anhand der übermittelten Adressendaten und ein Modifizieren der Adressendaten der im System vorhandenen lokalen Datenbanken anhand der aktualisierten Daten der Datenzentrale. Damit wird zwar ein Gleichhalten der Daten in jeder lokalen

Datenbank entsprechend einer zentralen Datenbank erreicht. Bei einer ungesicherten Verbindungsleitung kann aber nicht verhindert werden, daß eine unrichtige Adresse in der zentralen Datenbank der Datenzentrale gespeichert und von dort auf die jeweilige lokale Datenbank der weiteren Benutzer übertragen wird.

[0009] In der EP 782 296 A2 wurde zum Abrufen eines Zertifikates von einem Adressenbuchspeicher über eine ungesicherte Kommunikationsverbindung zwar ein Public Key-Verfahren vorgeschlagen, jedoch kann damit nur gesichert werden, daß die übermittelte Nachrich authentisch ist. Somit könnte ebensogut auch eine gefälschte Nachricht übermittelt werden, deren Zertifikat aber echt ist.

[0010] In frankierenden Systemen kommt es neben der Richtigkeit und Echtheit einer Nachricht zugleich auf die richtige Abrechnung an. Es ist deshab schon eine Portobox in einem Terminal (US 5,233,657) bzw. ein gesichertes Modul (US 5,625.694) vorgeschlagen worden, in welchem die Abrechnungsdaten gespeichert werden. Das Terminal gemäß der in der US 5,233,657 vorgeschlagenen Lösung, wird als Fax- und Frankiergerät genutzt, wobei wesentliche Frankierbilddaten von einer Datenzentrale angefordert werden und dann mit anderen Bilddaten, welche im Terminal gespeichert sind, als Frankierabdruck vervollständigt ausgedruckt werden. Die Kommunikation zwischen Terminal und Datenzentrale wird durch ein kryptographisches Verfahren gesichert, z.B. nach dem bekannten RSA-Verfahren. Aus den das Terminal kennzeichnenden Daten wird von der Zentralverarbeitungseinheit des Terminals ein Sicherungscode erzeugt und gemeinsam mit dem Frankierwert abgedruckt. Nachteilig ist die langwierige Rechenarbeit, welche die Zentralverarbeitungseinheit durchführen müß, einerseits wenn Bilddaten nach dem RSA-Verfahren entschlüsselt werden und andererseits wenn der Sicherungscode erzeugt wird.

[0011] In der US 5,625.694 wird ein Computer mit einem gesicherten Modul ausgerüstet. Bei einer Anforderung einer digitalen Unterschrift an ein solches gesichertes Modul, wobei die Anforderung in Abhängigkeit einer Änderung bezüglich des eingegebenen Frankierwertes und einer Empfängeradresse erfolgt, generiert das gesicherte Modul dann einerseits eine entsprechende digitale Unterschrift und übermittelt diese an den Mikroprozessor des Computers, aber führt andererseits auch die Abrechnung durch. Der Mikroprozessor des Computers generiert dann ein Druckbild entsprechend des Frankierwertes und der Empfängeradresse sowie der übermittelten Signatur. Eine Signatur wird nur dann nicht vom gesicherten Modul angefordert, wenn weder der Frankierwert noch die Adresse geändert wird. Eine Kopie desselben Abdruckes wird somit nicht im gesichertem Modul mitabgerechnet. Dem Postbeförderer obliegt die Authentizitätsprüfung für jedes einzelne Poststück. Auch geringste Unterschiede in der Adresse wirken sich auf die Signatur aus. Es ist jedoch nicht sicher, daß vom Benutzer die Eingabe einer gültigen Empfängeradresse erfolgt. Ein mit einer ungültigen Empfängeradresse versehenes Poststück kann u.U. nicht zugestellt werden, obwohl es mit einem gültigem Porto frankiert worden ist und das Porto ordnungsgemäß im gesicherten Modul abgerechnet wurde, weil die Adresse nachträglich nicht korrigierbar ist. Aufwendig ist bei allen vorgenannten Lösungen die Notwendigkeit der Anordnung eines gesicherten Moduls im Endgerät.

[0012] Aufgabe ist es, eine Low-end-Frankiereinrichtung mit einer lokalen Datenbank zu schaffen, wobei in der lokalen Datenbank der Frankiereinrichtung gültige Adressen gespeichert sind. Weiterhin soll ein Verfahren zur Erzeugung gültiger Daten für Frankierabdrucke angegeben werden, so daß im Ergebnis gültige Frankierwerte mit gültigen Adressen zusammen mit einer Signatur auf das Poststück gedruckt werden können.

[0013] Die Aufgabe wird mit den Merkmalen der Ansprüche 1 und 4 gelöst.

[0014] Die Notwendigkeit der Anordnung eines gesicherten Moduls im Endgerät entfällt. Damit entfällt auch die Notwendigkeit ein Guthaben in das Endgerät nachzuladen und die Kommunikation entsprechend sicher vor Manipulation des Guthabens zu gestalten. Erfindungsgemäß wird eine digitale Signatur in einer Datenzentrale eines Herstellers von Frankiersystemen bzw. eines Postbeförderers erzeugt. Die Kommunikation mit der Datenzentrale ist relativ kurz, da die übermittelten Klardaten weder Bilddaten umfassen noch alle Daten verschlüsselt werden, sondern neben den Klardaten nur eine relativ kurze Signatur zurückübermittelt wird. Vorteilhaft ist weiterhin die Dienstleistung der Datenzentrale bezüglich einer Korrektur einer fehlerhaft eingegeben-den Postempfängeradresse. Somit können Fehlfrankierungen vermieden werden. In einer Variante kann als zusätzliche Dienstleistung von der Datenzentrale eine Portoberechnung nach gültigem Tarif vorgenommen werden. Günstig ist auch für die Manipulationssicherheit, daß geheime Schlüssel und andere sicherheitsrelevante Daten nur in der Datenzentrale gespeichert sind und nach extern nicht ausgelesen werden können. Der Abdruck der übermittelten Daten auf daß Poststück kann auch zu einem beliebig späteren Zeitpunkt erfolgen. Für die externe Bilderzeugung aus den übermittelten Daten existieren keine Einschränkungen. So können unterschiedliche Druckverfahren zum Einsatz kommen. Den unterschiedlichen Einsatzbedingungen und Anforderungen der einzelnen Postbeförderer kann so am besten entsprochen werden.

[0015] Vorteilhafte Weiterbildungen der Erfindung sind in den Unteransprüchen gekennzeichnet bzw. werden nachstehend zusammen mit der Beschreibung der bevorzugten Ausführung der Erfindung anhand der Figuren näher dargestellt. Es zeigen:

Fig. 1, Blockschaltbild für die Frankiereinrichtung und die Datenzentrale,

Fig. 2, Beispiel für einen Abdruck auf einem Post-

stück.

[0016] Im Blockschaltbild gemäß Fig.1 ist eine Datenzentrale 20 mit Frankiereinrichtungen 10 und 30 und mit einer Prüfungsstelle 50, beispielsweise im Postamt, des Postbeförderers über ein Kommunikationsnetz 40 kommunikativ verbunden.

Die Frankiereinrichtung 10 ist als ein von einem ersten Computer 11 gesteuerter digitaler Drucker 17 ausgebildet, welcher mindestens Briefumschläge eines Formates bedrucken kann. Beispielsweise ist ein Personalcomputer PC 1 einerseits über ein ungesichertes Kabel 16 mit dem Drucker 17 verbunden und kann andererseits via Modem 15 und Kommunikationnetz 40 mit der Datenzentrale 20 on-line eine Kommunikationsverbindung aufnehmen. Mit dem ersten Computer 11 sind ein Festplattenspeicher 13 für eine lokale Datenbank, eine Tastatur 14 und eine Anzeigeeinheit 12 verbunden. Durch die letztgenannten Ein/Ausgabemittel 12 und 14 können entsprechende Eingaben getätigt und sichtbar gemacht bzw. die weitere Programmabarbeitung überwacht werden. Während der on-line Verbindung erfolgt eine Abstimmung des Datenbestandes der lokalen Datenbank und eine Speicherung der übermittelten Daten. Die Erzeugung von Abdrucken auf der Basis der übermittelten gespeicherten Daten kann zu einem späteren Zeitpunkt erfolgen.

[0017] Die Datenzentrale 20 besteht aus einem zweiten Computer 21, vorzugsweise ein Personalcomputer PC 2, mit angeschlossenen Ein/Ausgabemitteln 22 und 24, einer Festplatte 23 und mindestens einem Modem 25. Die Festplatte 23 speichert spezielle Dienstleistungsprogramme und Buchungs- bzw. Abrechnungsdaten für Dienstleistungen, welche für einen Kunden erbracht werden.

[0018] Auf die Festplatte 13 des ersten Personalcomputers PC 1 ist ein entsprechendes Anwendungsprogramm geladen, welches auf die Bedürfnisse der Benutzer für soho (smal office & home office) Märkte zugeschnitten ist. In einem solchen Markt kommt es nicht auf die Stückzahl frankierter Briefe pro Zeiteinheit an, sondern nur auf geringen Aufwand bei moderaten Kosten. Eine bloße Nachricht könnte zwar per email verschickt werden. Doch in der Praxis sollen auch unikate Orginale an Bildern, Fotos, Büchern, Stoffe usw. in einem Umschlag kuvertiert verschickt werden. Die Erfindung geht deshalb davon aus, daß das Grundsystem bestehend aus einem Computer und Drucker bereits beim Benutzer vorhanden ist. Nur dann kann im Endgerät auf zusätzliche und teure Hardware-Komponenten, beispielsweise auf ein Sicherheitsmodul, verzichtet werden, wenn das Frankiersystem entsprechend erfindungsgemäß ausgebildet ist. Der Computer muß zur Verarbeitung modemer Kryptotechnologien hardwaremäßig mit einem schnellen modernen Prozessor und genügend Speicherplatz ausgerüstet sein.

Die Erfindung setzt weiterhin vorraus, daß Kommunikationsverbindungen über das Netz 40, beispielsweise solche via Internet, WWW (Word Wide Web) oder ISDN, zukünftig kostengünstig hergestellt werden können.

[0019] Die Erfindung besteht darin, daß die Datenzentrale anhand einer auf der Festplatte 23 geschaffenen zentralen Datenbank die Gültigkeit einer Postempfängeradresse überprüft und gegebenenfalls herstellt, daß aber die Frankiereinrichtung vor einer Speicherung in der lokalen Datenbank die Authentizität einer übermittelten Postempfängeradresse überprüft. Dabei wird ein öffentlicher Schlüssel verwendet, welcher vorzugsweise zusammen mit der gültigen Postempfängeradresse und mit der Signatur von der richtigen Datenzentrale übermittelt wird. Keine andere als nur die richtige Datenzentrale kann die authentische Signatur erzeugen.

[0020] Die Überprüfung der Gültigkeit einer Adresse setzt eine Pflege der Adreßdateien der zentralen Datenbank durch einen Postbeförderer bzw. durch einen dazu vom Postbeförderer beauftragten Dienst vorraus. Zur Deckung der dadurch entstehenden Kosten wird die Nutzung der Adreßdateien durch externe Benutzer als kostenpflichtige Dienstleistung dem Benutzer in Anrechnung gebracht.

[0021] Zur Durchführung der Überprüfung wird mindestens die zu druckende Postempfängeradresse (Anschrift) zunächst an vorgenannte Datenzentrale übermittelt. Eine falsche Scheibweise der Anschrift kann automatisch anhand der Postleitzahl oder eines ähnlichen Bestimmungscode korrigiert werden, wenn zu letzterem eine entsprechende Datei in der zentralen Datenbank existiert. Das gilt auch umgekehrt. Ist jedoch eine automatische Korrektur nicht möglich, wird der Benutzer darüber informiert und aufgefordert die Adresse korrekt einzugeben. Nach der Überprüfung wird ein dem gültigen Tarif entsprechender Postwert und die gültige, eventuell zuvor korrigierte, Anschrift mit Postleitzahl an die Frankiereinrichtung zurückübermittelt, wobei die zurückübermittelten Daten mittels einer Signatur miteinander verknüpft sind. Als Zwischenschritt wird eine Nachricht aus den zu übermittelnden Daten erzeugt, indem eine spezielle mathematische Funktion zur Anwendung kommt, welche die zu verschlüsselnde Datenmenge reduziert. Die Signatur wird durch Verschlüsselung der Nachricht mit einem geheimen privaten Schlüssel nach einem bekannten nichtsymmetrischen Verschlüsselungsalgorithmus erzeugt.

[0022] Ein geeigneter bekannter asymmetrischer Verschlüsselungsalgorithmus ist beispielsweise der Digital Signatur Algorithmus(DSA), ein Elliptic Curve Digital Signatur Algorithmus (ECDSA) oder der ELGamal Algorithmus (ELGA). Diesen Signatur Algorithmen ist ein Schlüsselpaar gemeinsam, welches einen privaten und öffentlichen Schlüssel umfaßt. Der private Schlüssel ist ein geheimer nicht nach extern auslesbarer Schreibschlüssel. Und der öffentliche Schlüssel fungiert als Leseschlüssel für die Signatur und ist jederman zugänglich.

[0023] In der nicht vorveröffentlichten deutschen An-

meldung mit dem Titel: "Verfahren für eine digital druckende Frankiermaschine zur Erzeugung und Überprüfung eines Sicherheitsabdruckes", wurden derartige asymmetrische Verschlüsselungsalgorithmen auf "closed systems" angewendet näher erläutert. Auf der Frankiermaschinenseite wird jedoch im Unterschied zur erfindungsgemäßen Lösung ein Postage Security Device zur Verschlüsselung eingesetzt, das erfindungsgemäß nun entfallen kann.

[0024] Statt dessen hat die Festplatte 23 des zweiten Computers 21 der Datenzentrale 20 speziell gesicherte Speicherbereiche zur Speicherung des privaten Schlüssel, so daß letzterer nicht von extern ausgelesen werden kann. Alternativ kann ein separater Speicher, beispielsweise ein Halbleiterspeicher, zur sicheren Speicherung des privaten Schlüssels verwendet werden, wobei der Speicher im Computer integriert und gegen unberechtigtes Auslesen gesichert ist.

[0025] Es ist vorgesehen, daß der erste Computer 11 mittels eines Anwenderprogramms im Speicher programmiert ist, um

- auf eine gespeicherte bestimmte Postempfängeradresse zuzugreifen oder eine neu eingegebene bestimmte Postempfängeradresse zwischenzuspeichern,
- Anforderungsdaten des Postabsenders per Kommunikationsmittel zur Datenzentrale zu übermitteln, wobei die Anforderungsdaten die Identifikationsdaten des Postabsenders und Postversendungsdaten, einschließlich die bestimmte Postempfängeradresse, umfassen, um die Richtigkeit der Postempfängeradresse mittels eines zweiten Computers zu bestätigen oder anhand einer in der zentralen Datenbank gespeicherten Adreßdatei herzustellen,
- Daten zu empfangen, betreffend eine gültige Postempfängeradresse von einer in der zentralen Datenbank gespeicherten Adreßdatei, einen gültigen Portowert und eine Signatur, wobei der zweite Computer der Datenzentrale die angeforderten Daten nur mit einer Signatur ausstattet, wenn eine gültige Postempfängeradresse in der zentralen Datenbank gespeichert ist, wobei eine Mitteilung erzeugt wird, wenn eine automatische Korrektur einer Postempfängeradresse unmöglich ist,
- die von der zentralen Datenbank empfangenen Daten einschließlich der Signatur zu verarbeiten, um einen authentischen Frankierabdruck auf das Poststück abzudrucken.

Es ist weiterhin vorgesehen, die Authentizität der zur Frankiereinrichtung übermittelten empfangenen Daten anhand der Signatur zu überprüfen und bei Authentizität die Adreßdatei in der lokalen Datenbank bezüglich der bestimmte Postempfängeradresse zu aktualisieren.

[0026] Das erfindungsgemäße Verfahren zur Erzeugung eines gültigen Datenbestandes für Frankierabdrucke umfaßt folgende Schritte:

- Bildung und Übermittlung von Anforderungsdaten, mit welchen ein erster Computer der Frankiereinrichtung von einem zweiten Computer einer Datenzentrale eine Signatur anfordert, wobei die Anforderungsdaten mindestens eine Informationsgruppe mit Postempfängeradressendaten und Identifikationsdaten einschließen,
- Erzeugung einer Signatur auf der Basis verifizierter Daten unter Verwendung eines asymmetrischen Kryptoalgorithmus und geheimen privaten Schlüssels, sowie
- Rückübermittlung der verifizierten Daten und der Signatur zur Frankiereinrichtung, wobei die Authentizität der zurückübermittelten Daten anhand der Signatur unter Verwendung eines öffentlichen Schlüssels überprüfbar ist, sowie
- Speicherung authentischer empfangener Daten in einer lokalen Datenbank.

[0027] Es ist vorgesehen, daß vom zweiten Computer in der Datenzentrale die Gültigkeit von Daten überprüft und erforderlichenfalls hergestellt wird, daß die Signatur vom zweiten Computer in der Datenzentrale aus den angeforderten Daten generiert wird. Somit ist sichergestellt, daß die vom Endgerät empfangenen teilweise zurückzuübermittelnden gültigen Daten vom zweiten Computer in der Datenzentrale mittels der Signatur miteinander verknüpft worden sind. Der erste Computer empfängt entsprechend der Anforderung über Modem somit gültige Daten. Es ist weiterhin vorgesehen, daß vom ersten Computer anhand von Daten der zur Datenzentrale übermittelten Informationsgruppe und Daten einer empfangenen Informationsgruppe ein Vergleich vorgenommen wird, wobei mittels der Signatur eine Authentizitätsprüfung hinsichtlich der empfangenen Informationsgruppe durchgeführt wird, wobei bei der Authentizitätsprüfung ein öffentlicher Schlüssel verwendet wird, welcher in der zentralen oder einer lokalen Datenbank abrufbar gespeichert ist.
Im Falle einer festgestellten Abweichung zwischen den übermittelten und empfangenen Daten im Ergebnis des Vergleiches wird der Datenbestand in der lokalen Datenbank nur dann aktualisiert, wenn die empfangenen Daten als authentisch gelten. Vom ersten Computer wird dann zu einem beliebig späteren Zeitpunkt aus den empfangenen Daten ein Druckbild generiert und ein Ausdrucken entsprechend veranlaßt.

[0028] Dem Gleichhalten der Postempfängeradreßdaten in der lokalen Datenbank geht also eine Authentizitätsprüfung anhand der Signatur im Personalcomputer PC 1 voraus. Bei der Authentizitätsprüfung wird ein öffentlicher Schlüssel verwendet, welcher von der zentralen oder einer lokalen Datenbank abrufbar ist. Der öffentliche Schlüssel kann in einem ungesicherten Speicherbereich zusammen mit einem zugehörigem Datum für das Gültigwerden gespeichert werden.

[0029] Mit dem öffentlichen Schlüssel kann jederman aus der Signatur durch Entschlüsseln die Nachricht zurückgewinnen. Zwecks Vergleich wird eine Referencenachricht aus den übermittelten Klardaten erzeugt, indem die dieselbe vorgenannte spezielle mathematische Funktion zur Anwendung kommt, welche die Datenmenge reduziert. Bei Gleichheit der entschlüsselten Nachricht mit der gebildeten Referencenachricht ist die Authentizität der Daten gegeben, deren Gültigkeit durch die Datenzentrale zumindest für die Postempfängeradresse gesichert wird.

[0030] Auf ebensolche Weise kann anhand der Signatur in einem Postamt 50 oder in einer Posteinlieferungsstelle bzw. einem Institut eines privaten Postbeforderers mit der Authentizitätsprüfung zugleich überprüft werden, ob eine Abrechnung in der Datenzentrale erfolgt ist. Zu diesem Zweck geht in die Signatur eine monoton stetig veränderbare Größe ein, welche zugleich in Klarschrift auf dem Poststück offen aber mindestens maschinenlesbar abgedruckt wird. Eine solche Größe sind beispielsweise die Zeitdaten zum Zeitpunkt des Abrufens der Signatur von der zentralen Datenbank oder die Stückzahl. Zugleich werden anhand der aufgedruckten Zeitdaten bzw. Stückzahl oder einer anderen Größe in der Datenzentrale die Buchhaltungsdaten wiederauffindbar und somit die Bezahlung der Dienstleistung im Detail überprüfbar.

[0031] Das Postamt 50 bzw. beauftragte Institut kann dazu die Datenzentrale via Kommunikationverbindung anrufen, um in deren Datenbank gespeicherte Daten abzufragen.

[0032] Ein Beispiel für einen Abdruck auf einem Poststück wird anhand der Fig. 2 erläutert. Bei einem Brief ist das Adreßfeld zentral angeordnet. Die Postempfängeradersse wird in Klarschrift und ein zugehöriger ZIP-Code wird als Barcode aufgedruckt. Der Frankierabdruck ist in der Peripherie rechts oben angeordnet. Eine Absenderangabe in der Peripherie links oben angeordnet ist optional. Für die USPS wird ein ca. 1 Zoll breiter Frankierabdruck mit einem maschinenlesbaren Bereich erzeugt. Bestimmte Klardaten und die Signatur werden z.B. in eine PDF 417-Symbolik umgesetzt und gedruckt. Letztere ist von der Firma Symbol Technologies, inc. in EP 439 682 B1 näher beschrieben worden. Über dem maschinenlesbaren Bereich ist der visuell (human) lesbare Bereich und ein Bereich für den FIM-Code gemäß der US-Postvorschriften angeordnet. Links davon liegt ein weiterer Druckbereich, welcher vorzugsweise zum Drucken eines Werbeklischees verwendet werden kann. Wegen des FIM-Codes ergibt sich für einen ca. 1 Zoll breiten Frankierabdruck ein ca 11 bis 14 mm breiter visuell (human) lesbarer Bereich. Somit kann die restliche Breite für den maschinenlesbaren Bereich verwendet werden.

[0033] Die zur Datenzentrale übermittelten Anforderungsdaten können in einer bevorzugten ersten Ausführungsvariante zusätzlich den Postwert, weitere Postversendungsdaten und eine monoton stetig veränderbare Größe einschließen. Der Postwert und weitere Postversendungsdaten (EXPRESS, AIR MAIL,..,) werden über die Tastatur 14 des Personalcomputers PC 1 vom Benutzer für jeden Brief eingegeben.

[0034] Die Speicherung der Abrechnung bzw. Buchhaltungsdaten entsprechend weiterer Dienstleistungen erfolgt in der zentralen Datenbank. Da die Abrechnung der Postbeförderung in der Datenzentrale kundenspezifisch vorgenommen wird, kann eine Manipulation der Abrechnungsdaten in Fälschungsabsicht ausgeschlossen werden. Eine lokale Portobox bzw. ein Meter ist beim Benutzer der Frankiereinrichtung unnötig. Die Festplatte 23 enthält zur Buchung vorgesehene Speicherbereiche, entsprechend der vereinbarten Abrechnungsart und Dienstleistungsart. Zur Erhöhung der Sicherheit vor Datenverlust existiert mindestens eine weitere - nicht gezeigte - Festplatte 23' in der Datenzentrale, in welcher eine redundante Speicherung aller Daten erfolgt.

[0035] Eine Abrechnungsart für vorgenannten Dienstleistung der Postbeförderung ist eine kumulative Abrechnung am Monatsende, wobei der kumulative Betrag von einem Kundenkonto bei einer Bank oder einem vergleichbaren Kreditinstitut gemäß dem Lastschriftverfahren abgebucht wird. Es kann ebenso eine andere Abrechnungsart, beispielsweise Sofortbezahlung oder Vorausbezahlung, vereinbart werden. Mit dem Kunden kann eine entsprechende Vereinbarung zu unterschiedlichen Abrechnungsarten für unterschiedliche Dienstleistungen getroffen werden.

[0036] Es ist in einer zweiten Ausführungsvariante vorgesehen, daß Versendungsdaten übermittelt und außerdem die Dienstleistung einer Portoberechnung in der Datenzentrale durchgeführt wird, wobei die kumulierten Dienstleitungskosten periodisch, beispielsweise am Tagesende, dem Kunden in Rechnung gestellt werden. Dazu ist es vorteilhaft, daß die Anforderungsdaten, welche zusammen mit der Adreßdaten und weiteren Versendungsdaten zur Datenzentrale übermittelt werden, auch Identifikationsdaten ID umfassen. Unter Identifikationsdaten ID sollen eine Identifikationsnummer des Kunden bzw. des Postabsenders oder die Maschinenseriennummer, oder die Absendeadresse verstanden werden. Um Betrügereien auszuschließen, wo ein anderer Absender vorgetäuscht wird, ist es weiterhin vorgesehen, daß solche Identifikationsdaten in die Signatur ebenfalls mit eingehen. Die Datenzentrale erzeugt eine Signatur aus den übermittelten Anforderungsdaten, wie Postempfängeradresse und Identifikationsdaten, sowie einer erzeugten monoton stetig veränderbare Größe und dem Portowert mit Hilfe eines privaten Schlüssels und eines asymmetrischen Verschlüsselungsalgorithmus.

[0037] Wenn aber andererseits wie bei der ersten Ausführungsvariante die Dienstleistung einer Portoberechnung nicht in der Datenzentrale sondern in der Frankiereinrichtung durchgeführt wird, können solche Kosten nicht dem Kunden aufgebürdet werden, sondern

vielmehr ist ein Rabatt zu gewähren, da der Computer der Datenzentrale durch solche Berechnungen nicht unnötig blockiert wird.

[0038] Bei der zweiten Ausführungsvariante ist vorgesehen, daß die empfangenen teilweise zurückübermittelten Daten einen in der Datenzentrale berechneten Portowert, eine Empfänderadresse, Identifikationsdaten, Datenzentrale eine monoton stetig veränderbare Größe und eine Signatur einschließen, wobei die Datenzentrale die monoton stetig veränderbare Größe generiert und aus den übermittelten Anforderungsdaten, wie Postempfängeradresse und Identifikationsdaten sowie aus weiteren übermittelten Versendungsdaten den Portowert nach einem gültigen Tarif ermittelt. Bei einer Maximalvariante werden die Anforderungsdaten gleich für mehrere Briefe erzeugt, die der Benutzer an seinem Personalcomputer PC 1 erstellt hat, welcher zugleich Bestandteil der Frankiereinrichtung ist. Entsprechend der Anzahl der Briefe wird dann auch eine Anzahl von verschiedenen Signaturen zugeordnet zu den Adreß- und Frankierdaten erzeugt. Die zurückübermittelten Daten lassen sich über die Adreßdaten den unschiedlichen Briefen zuordnen.

[0039] Als alternative Versendungsinformation zum Gewicht kann die Anzahl und das Format und das Gewicht der einzelnen Briefseiten je Brief übermittelt werden. Das Briefgewicht läßt sich daraus in der Datenzentrale ermitteln, ohne daß beim lokalen Benutzer eine Briefwaage an die Frankiereinrichtung angeschlossen werden muß. Gegebenenfalls eröffnet die Datenzentrale während der Kommunikation einen Userdialog via dem Display 12 mit dem Benutzer, um die Daten zu vervollständigen, welche zur Portoberechnung erforderlich sind.

[0040] Bei einer Minimalvariante, wird lediglich eine Signatur für folgende Informationen Postempfängeradresse, Postwert, Identifikationsdaten, Stückzahlwert angefordert. Der Stückzahlwert ist ein durch einen Numerateur erzeugter unverschlüsselter Stückzahlaufdruck. Durch einen Numerateur wird bereits ein hinreichender Schutz gegenüber Kopien des Abdruckes erreicht. Bei Abholung der gesammelten Post durch einen Angestellten des Postbefördereres könnten bereits die Absender-Identifikationsdaten und der vom Numerateur erreichte Zählstand mit den aufgedruckte Werten verglichen werden.

[0041] Die Wahrscheinlichkeit ist auch dafür gering, daß zum selben Absendedatum ein gleich großes und gleich schweres Poststück an den selben Postempfänger geschickt wird. Die Wahrscheinlichkeit kann weiter verringert werden, indem gefordert wird, daß die Uhrzeitdaten zusätzlich auf das Poststück mit aufgedruckt werden. Die Zeitdaten können alternativ durch eine genaue Uhr - nicht gezeigt - von der Datenzentrale bereitgestellt werden.

[0042] Es ist in einer weiteren Variante vorgesehen, daß alle auf das Poststück aufzudruckenden Daten zuvor zentral gespeichert werden. In dem Postamt kann die eingelieferte Post unter Mitwirkung der zentral gespeicherten Daten daraufhin überprüft werden, ob Kopien eines Abdruckes in Fälschungsabsicht benutzt werden. Zu jedem eingelieferten Poststück kann ein Eintrag in der zentralen Datenbank in einem besonderen Bereich vorgenommen werden. Ein doppelter Eintrag in der Datenbank deutet dann auf einen gefälschten Abdruck hin. Durch die Verknüpfung der Postempfängeradresse mit dem Postwert und Stückzahl über die Signatur, ist es getrennt voneinander unmöglich, eines der beiden Postempfängeradresse bzw. Postwert für Manipulationzwecke zu kopieren.

[0043] Es ist weiterhin vorgesehen, daß ein jedes Schlüsselpaar, bestehend aus einem privaten Schlüssel und einem öffentlichen Schlüssel, zeitlich limitiert gültig ist und plötzlich zu einem bestimmten Datum und Uhrzeit von der Datenzentrale gewechselt werden kann. Die zeitlichen Abstände des Wechselns ergeben sich entsprechend dem aktuell erreichten Fortschritten bei modernen Analyseverfahren, beispielsweise der differenziellen Kryptoanalyse, und sind so bemessen, daß ein Angriff auf die Sicherheit des Systems mit hoher Wahrscheinlichkeit scheitern muß.

[0044] Die Erfindung ist nicht auf die vorliegenden Ausführungsform beschränkt, da offensichtlich weitere andere Anordnungen bzw. Ausführungen der Erfindung entwickelt bzw. eingesetzt werden können, die vom gleichen Grundgedanken der Erfindung ausgehend, die von den anliegenden Ansprüchen umfaßt werden.

Patentansprüche

1. Frankiereinrichtung, mit einem ersten Computer und mit einem angeschlossenen Drucker, wobei der Computer einen Speicher mit einer lokalen Datenbank für Postempfängeradreßdateien und ein Kommunikationsmittel enthält, wobei der erste Computer über das Kommunikationsmittel mit einer Datenzentrale verbunden ist, welche einen zweiten Computer mit einer zentralen Datenbank aufweist, **gekennzeichnet dadurch**, daß der erste Computer programmiert ist,

   - auf eine gespeicherte bestimmte Postempfängeradresse zuzugreifen oder eine neu eingegebene bestimmte Postempfängeradresse zwischenzuspeichern,
   - Anforderungsdaten des Postabsenders per Kommunikationsmittel zur Datenzentrale zu übermitteln, wobei die Anforderungsdaten die Identifikationsdaten des Postabsenders und Postversendungsdaten, einschließlich die bestimmte Postempfängeradresse, umfassen, um die Richtigkeit der Postempfängeradresse mittels des zweiten Computers zu bestätigen oder anhand einer in der zentralen Datenbank gespeicherten Adreßdatei herzustellen,

- Daten zu empfangen, betreffend eine gültige Postempfängeradresse von einer in der zentralen Datenbank gespeicherten Adreßdatei, einen gültigen Portowert und eine Signatur, wobei der zweite Computer der Datenzentrale die angeforderten Daten nur mit einer Signatur ausstattet, wenn eine gültige Postempfängeradresse in der zentralen Datenbank gespeichert ist, wobei eine Mitteilung erzeugt wird, wenn eine automatische Korrektur einer Postempfängeradresse unmöglich ist,
- die von der zentralen Datenbank empfangenen Daten einschließlich der Signatur zu verarbeiten, um einen authentischen Frankierabdruck auf das Poststück abzudrucken.

2. Frankiereinrichtung, nach Anspruch 1, **gekennzeichnet dadurch,** daß der erste Computer weiterhin programmiert ist, die Authentizität der zur Frankiereinrichtung übermittelten empfangenen Daten anhand der Signatur zu überprüfen und bei Authentizität die Adreßdatei in der lokalen Datenbank bezüglich der bestimmte Postempfängeradresse zu aktualisieren.

3. Frankiereinrichtung, nach Anspruch 1, **gekennzeichnet dadurch,** daß der erste Computer weiterhin programmiert ist, die Anforderungsdaten zu bilden, wobei die Postversendungsdaten den gewünschten Frankierwert einschließen.

4. Verfahren zur Erzeugung gültiger Daten für Frankierabdrucke, wobei von einer Frankiereinrichtung Anforderungsdaten gebildet und zu einer Datenzentrale übermittelt und angeforderte Daten zurückübermittelt und gespeichert werden, **gekennzeichnet durch** die Schritte:

   - Bildung und Übermittlung von Anforderungsdaten, mit welchen ein erster Computer der Frankiereinrichtung von einem zweiten Computer einer Datenzentrale eine Signatur anfordert, wobei die Anforderungsdaten mindestens eine Informationsgruppe mit Postempfängeradressendaten und Identifikationsdaten einschließen,
   - Verifikation von übermittelten Daten in einer Datenzentrale,
   - Erzeugung einer Signatur auf der Basis verifizierter Daten unter Verwendung eines asymmetrischen Kryptoalgorithmus und geheimen privaten Schlüssels, sowie
   - Rückübermittlung der verifizierten Daten und der Signatur zur Frankiereinrichtung, wobei die Authentizität der zurückübermittelten Daten anhand der Signatur unter Verwendung eines öffentlichen Schlüssels überprüfbar ist, sowie
   - Speicherung authentischer empfangener Daten in einer lokalen Datenbank.

5. Verfahren, nach Anspruch 4, **gekennzeichnet dadurch,**

   - daß vom zweiten Computer in der Datenzentrale die Gültigkeit von Daten überprüft und erforderlichenfalls hergestellt wird, daß die Signatur vom zweiten Computer in der Datenzentrale aus den angeforderten Daten generiert wird, wobei die teilweise zurückzuübermittelnden Daten vom zweiten Computer in der Datenzentrale mittels der Signatur miteinander verknüpft werden,
   - daß der erste Computer entsprechend der Anforderung über Modem gültige Daten empfängt,
   - daß vom ersten Computer anhand von Daten der zur Datenzentrale übermittelten Informationsgruppe und Daten einer empfangenen Informationsgruppe ein Vergleich vorgenommen wird, wobei mittels der Signatur eine Authentizitätsprüfung hinsichtlich der empfangenen Informationsgruppe durchgeführt wird, wobei bei der Authentizitätsprüfung ein öffentlicher Schlüssel verwendet wird, welcher in der zentralen oder einer lokalen Datenbank abrufbar gespeichert ist,
   - daß im Falle einer festgestellten Abweichung zwischen den übermittelten und empfangenen Daten im Ergebnis des Vergleiches der Datenbestand in der lokalen Datenbank nur dann aktualisiert wird, wenn die empfangenen Daten als authentisch gelten, sowie
   - daß vom ersten Computer aus den empfangenen Daten ein Druckbild generiert und ein Ausdrucken entsprechend veranlaßt wird.

6. Verfahren, nach Anspruch 5, **gekennzeichnet dadurch,** daß die zur Datenzentrale übermittelten Anforderungsdaten zusätzlich den Postwert, weitere Postversendungsdaten und eine monoton stetig veränderbare Größe einschließen.

7. Verfahren, nach Anspruch 5, **gekennzeichnet dadurch,** daß die empfangenen teilweise zurückübermittelten Daten einen in der Datenzentrale berechneten Portowert, eine Empfänderadresse, Identifikationsdaten, Datenzentrale eine monoton stetig veränderbare Größe und eine Signatur einschließen, wobei die Datenzentrale die monoton stetig veränderbare Größe generiert und aus den übermittelten Anforderungsdaten, wie Postempfängeradresse und Identifikationsdaten sowie aus weiteren übermittelten Daten den Portowert nach einem gültigen Tarif ermittelt, sowie aus den übermittelten Anforderungsdaten, wie Postempfängeradresse und Identifikationsdaten, sowie der erzeugten mo-

noton stetig veränderbare Größe und dem Portowert mit Hilfe eines privaten Schlüssels und eines asymmetrischen Verschlüsselungsalgorithmus eine Signatur erzeugt.

8. Verfahren, nach den Ansprüchen 6 oder 7, **gekennzeichnet dadurch**, daß die monoton stetig veränderbare Größe eine zeitbezogene Größe ist.

9. Verfahren, nach den Ansprüchen 6 oder 7, **gekennzeichnet dadurch**, daß die monoton stetig veränderbare Größe eine Stückzahl an abgerechneten Poststücken ist.

10. Verfahren, nach den Ansprüchen 4 und 5 oder 7, **gekennzeichnet dadurch**, daß ein jedes Schlüsselpaar aus privaten Schlüssel und einem öffentlichen Schlüssel zeitlich limitiert gültig ist und plötzlich zu einem bestimmten Datum und Uhrzeit von der Datenzentrale gewechselt werden kann.

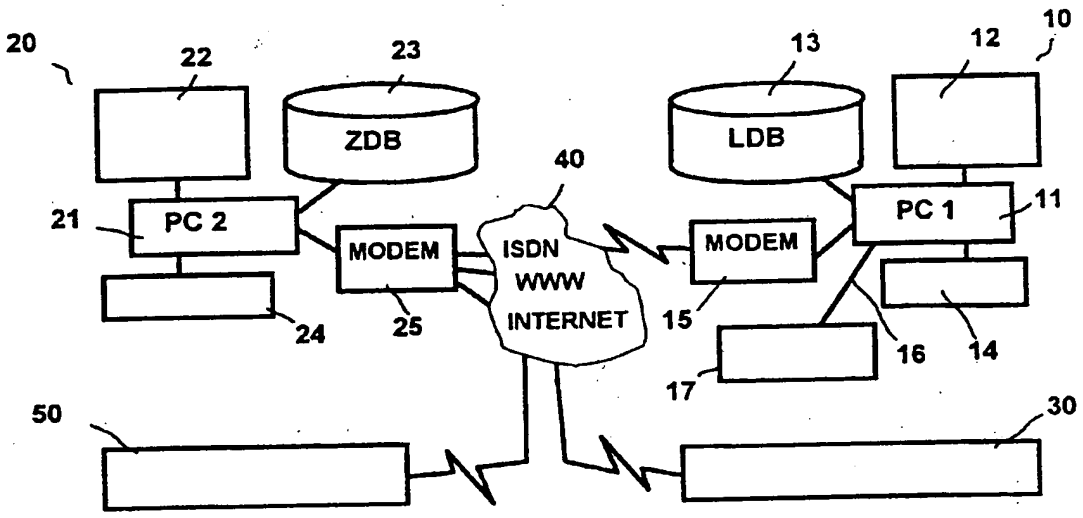
20
22
23
ZDB
13
LDB
12
10
40
21
PC 2
MODEM
ISDN
WWW
INTERNET
MODEM
PC 1
11
24
25
15
16
14
17
50
30

Fig.1

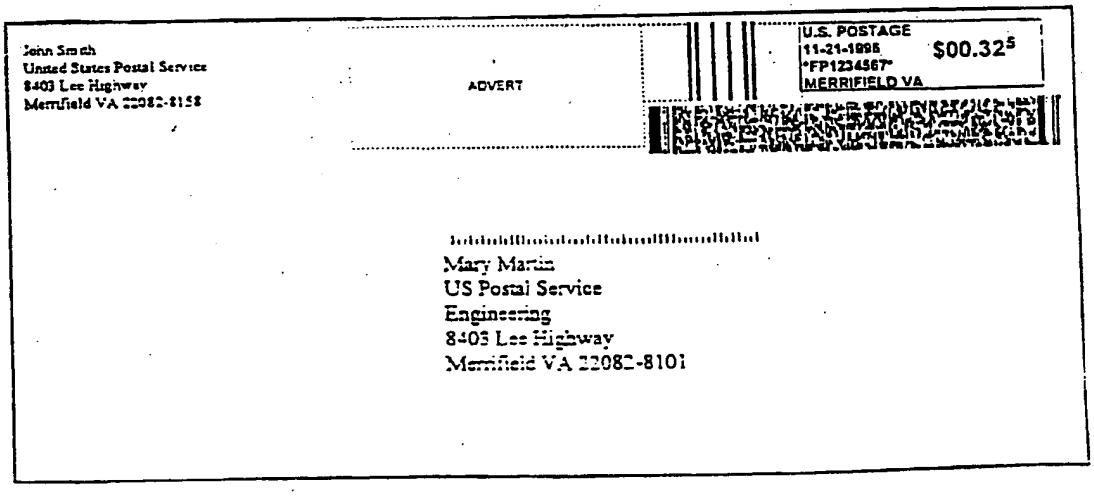
John Smith
United States Postal Service
8403 Lee Highway
Merrifield VA 22082-8158
ADVERT
U.S. POSTAGE
11-21-1998
FP1234567
MERRIFIELD VA
$00.32
Mary Martin
US Postal Service
Engineering
8403 Lee Highway
Merrifield VA 22082-8101

Fig. 2